3000 AWARENESS

This section of the AMS Plan details how rapid access to vital information will be given to Northeast and Eastern Central Florida critical decision makers during routine and crisis maritime situations. The section is organized as follows:

3100 (U) Introduction

The AMS Plan is the fundamental element in building vigilant "Situational Awareness" and is key to the successful development of the Maritime Domain Awareness program. It will serve to assist the United States Department of Homeland Security in producing a "common operations picture" (COP) of the maritime environment. The AMS Plan affords rapid access to vital information by critical decision makers within the area maritime community during routine and crisis maritime situations.

3200 (SSI) Federal, State & Local Security & Law Enforcement Agency Jurisdiction

TABLE 3200.1: First Tier Agencies (SSI)
Police, fire and emergency medical units normally dispatched thru the e-911 system

Agency	Jurisdictional Limits	Installation Locations	Capabilities
United States Coast Guard Group Mayport (904) 247-7311	(RESERVED)	Station Mayport FL	[SSI Information Removed]
		Station Ponce Inlet FL	[SSI Information Removed]
		Station Port Canaveral	[SSI Information Removed]
		CGC KINGFISHER	[SSI Information Removed]
		CGC SHRIKE	[SSI Information Removed]
		CGC MARIA BRAY	[SSI Information Removed]
United States Coast Guard Marine Safety Office (904) 247-7318	Defined at 33 CFR part Sec. 3.35-20.	Jacksonville FL	[SSI Information Removed]
		Port Canaveral FL	[SSI Information Removed]
Bureau of Customs and Border Protection	(RESERVED)	Jacksonville FL	[SSI Information Removed]
	(RESERVED)	Port Canaveral FL	[SSI Information Removed]
Immigration and Customs Enforcement		Jacksonville	[SSI Information Removed]
	(RESERVED)	Port Canaveral	[SSI Information Removed]

U.S. FWS		Jacksonville	[SSI Information Removed]
Florida Department of Law Enforcement	Defined at Chapter 943 Florida Statutes	Seven (7) FDLE Regional Operation Centers located in the following cities: Jacksonville, Orlando, Tallahassee, Pensacola, Tampa, Ft Myers and Miami. Additional Field Offices are strategically located throughout the State of Florida. Jacksonville/Orlando	[SSI Information Removed]
Florida Fish and Wildlife Conservation Commission	(RESERVED)	Jacksonville/Orlando	[SSI Information Removed]
Nassau County Sheriffs	(RESERVED)	(RESERVED)	[SSI Information Removed]
Fernandina Beach Police Department	(RESERVED)	(RESERVED)	[SSI Information Removed]
Jacksonville Sheriff's Office	(RESERVED)	(RESERVED)	[SSI Information Removed]
Jacksonville Fire and Rescue	(RESERVED)	(RESERVED)	[SSI Information Removed]
Atlantic Beach Police Department	(RESERVED)	(RESERVED)	[SSI Information Removed]
Neptune Beach Police Department	(RESERVED)	(RESERVED)	[SSI Information Removed]
Jacksonville Beach Police Department	(RESERVED)	(RESERVED)	[SSI Information Removed]
CSX Railway Police	(RESERVED)	(RESERVED)	[SSI Information Removed]
Brevard County Sheriffs	(RESERVED)	(RESERVED)	[SSI Information Removed]
Port Canaveral Police Department	(RESERVED)	(RESERVED)	[SSI Information Removed]
Port Canaveral Fire Department	(RESERVED)	(RESERVED)	[SSI Information Removed]
Cocoa Beach Fire Department	(RESERVED)	(RESERVED)	[SSI Information Removed]

Table 3200.2: Second Tier Agencies

Agencies with special recovery and containment capabilities in dealing with hazardous materials, rough terrain and underwater search and recovery. Other units may be excavation or heavy equipment capable.

Agency	Jurisdictional Limits	Installation Locations	Capabilities
		Jacksonville FL	[SSI Information Removed]

United States Coast Guard Marine Safety Office (904) 247-7311	Defined at 33 CFR part Sec. 3.35-20.	Jacksonville FL	[SSI Information Removed]
United States Coast Guard Gulf Strike Team Marine Safety Office (123) 123-1234	(RESERVED)	(RESERVED) Port Canaveral FL	[SSI Information Removed]
United States Coast Guard Maritime Safety and Security Team 91109 (123) 123-1234	When deployed to the Northeast and Eastern Central Florida Area, the MSST operates under the jurisdiction of the U.S. Coast Guard Marine Safety Office.	St. Marys, GA	[SSI Information Removed]
Federal Bureau of Investigation	(RESERVED)	Jacksonville Regional Office	[SSI Information Removed]
	(RESERVED)	Orlando Regional Office	[SSI Information Removed]
Naval Criminal Investigative Service	(RESERVED)	Jacksonville	[SSI Information Removed]
Federal Railroad Adminstration	(RESERVED)	Jacksonville	[SSI Information Removed]
Joint Terrorism Task Force	(RESERVED)	Jacksonville	[SSI Information Removed]
Regional Domestic Security Task Force	(RESERVED)	Jacksonvill	[SSI Information Removed]
High Intensity Drug Trafficking Area	(RESERVED)	Jacksonville	[SSI Information Removed]
Field Intelligence Support Team	(RESERVED)	Jacksonville	[SSI Information Removed]
Florida Nat.Guard Civil Support Team	(RESERVED)	Jacksonville	[SSI Information Removed]

Table 3200.3: Third Tier Agencies
the National Guard, Military Reserve and other national level response elements.

Agency	Jurisdictional Limits	Installation Locations	Capabilities
United States Coast Guard Group Mayport RESERVE FORCES (904) 247-7311	(RESERVED)	Station Mayport FL	[SSI Information Removed]
		Station Ponce Inlet FL	[SSI Information Removed]
		Station Port Canaveral	[SSI Information Removed]
		CGC KINGFISHER	[SSI Information Removed]
		CGC SHRIKE	[SSI Information Removed]
		CGC MARIA BRAY	[SSI Information Removed]
		Jacksonville FL	[SSI Information Removed]

United States Coast Guard Marine Safety Office RESERVE FORCES (904) 247-7311	Defined at 33 CFR part Sec. 3.35-20.	Jacksonville FL	[SSI Information Removed]
Florida National Guard (123)123-1234	(RESERVED)	Florida Port Canaveral FL	[SSI Information Removed]
FBI HRT	(RESERVED)	Jacksonville	[SSI Information Removed]
DOE RAP TEAM	(RESERVED)	Jacksonville	[SSI Information Removed]

3300 (U) Area Maritime Security (AMS) Assessment

This Area Maritime Security Assessment is organized as follows:

3310 (U) Introduction

The Port Security Committees for the Northeast and Eastern Central Florida have created this Area Maritime Security Assessment (AMSA) to provide strategies, tactics, techniques, and procedures for the protection and defense of the United States Marine Transportation System (MTS) from smuggling, thievery, illegal protest, and terrorism. This AMSA has been undertaken in accordance with requirements of Title 33 Code of Federal Regulations part 103 and the guidance in Coast Guard Navigation and Vessel Inspection Circular 11-02.

3320 (SSI) Critical Marine Transportation Infrastructure and Operations

[SSI Information Removed]

3330 (SSI) Area Maritime Security Threat Assessment

[SSI Information Removed]

3340 (SSI) Area Maritime Security Assessment

[SSI Information Removed]

3350 (SSI) Security Measures for MARSEC 1, 2, and 3

[SSI Information Removed]

3400 (U) Communications

Communication is a vital function for prevention operations and incident responses. An understanding of communication methodology, programs, processes, and physical attributes is essential to all personnel involved in the security process. This section outlines the means by which communication under this plan will occur. The section is organized as follows (click the link to view the subsection):

3410 (U) Communication of Security Information

Security informational needs are multilayered with a large variety of stakeholder requirements or needs. The next sections will identify methodology used to communicating security information.

The Port Security Committees and the Maritime Joint Task Force have developed a communication plan using the P-A-C-E method. This method can be used for routine or crisis situations and will be tested periodically to ensure connectivity.

- **P** Primary system of contact for disseminating information.
- **A** Alternate system of contact (can be same method as primary but on a different frequency or phone number).
- **C** Contingency system is used when both the primary and alternate are not effective.
- **E** Emergency is the most failsafe and should be used in a real emergency or when the other systems are not successful.

Section 3500 of this plan contains information pertaining to the protection and dissemination of SSI.

3410 (U) Communication of Security Information

Security informational needs are multilayered with a large variety of stakeholder requirements or needs. The next sections will identify methodology used to communicating security information.

The Port Security Committees and the Maritime Joint Task Force have developed a communication

plan using the P-A-C-E method. This method can be used for routine or crisis situations and will be tested periodically to ensure connectivity.

- **P** Primary system of contact for disseminating information.
- **A** Alternate system of contact (can be same method as primary but on a different frequency or phone number).
- **C** Contingency system is used when both the primary and alternate are not effective.
- **E** Emergency is the most failsafe and should be used in a real emergency or when the other systems are not successful.

Section 3500 of this plan contains information pertaining to the protection and dissemination of SSI.

3410.1 (U) Communication with the Public

The public as whole must be notified of events and operations that might affect them. There are a variety of systems that may be used to communicate information on restrictions, closures, and activities that are exclusionary or restrictive in nature.

Table 3410.1-1: (U) Communication to the General Public

Information to Communicate	Who communicates	How the Information Is Communicated	When the Information Is Communicated
Homeland Security Advisory System (HSAS) Threat Advisory Level and specific waterway closures linked to the HSAS Threat Level.	Department of Homeland Security	**P -** Via major media outlets.	Within DHS-established timeframes related to the decision to change the HSAS level.
	Coast Guard Integrated Command Center	**A -** Through electronic distribution of a Marine Safety Information Bulletin (MSIB) via e-mail and posting on the MSO Jacksonville, GRU Mayport, JMTX, and Canaveral Port Authority Internet web pages; a volunteer subscription list is contained in Tab G to Appendix 9500 – interested waterway users may subscribe or delete their addresses from this list on a continuous basis. See Enclosure (X) to Tab A to Appendix 9500.	Within 2 Hours of HSAS level changes and associated waterway closures.
	Coast Guard Integrated Command Center	**C -** Recurring Boadcast Notice to Mariners issued on Channel 16. See Enclosure (X) to Tab A to Appendix 9500.	Within 2 Hours of MARSEC level changes and associated waterway closures.
	County Emergency Operations Centers	**E -** Emergency evacuation/alert phone calls and Emergency Broadcast System alerts.	In extreme emergencies when the public must be directly informed in order to protect lives, within DHS-established timeframes.

Table 3410.1-1: (U) Communication to the General Public (continued)

Information to Communicate	Who communicates	How the Information Is Communicated	When the Information Is Communicated
Marine and Special Shoreline Event restrictions that could bear on attendees.	USCG MSO Jacksonville	**P -** In the publicly available Unclassified version of the Area Maritime Security Plan posted on the Marine Safety Office Jackonville Internet. See the 4000 Series – PREVENTION.	Not later than 01 July 2004 and updated at least annually.
	USCG MSO Jacksonville, GRU Mayport, JMTX, and Canaveral Port Authority	**A –** Published in Title 33 Code of Federal Regulations part 165 and the Federal Register.	Before activation for standing security zones and as soon as possible for emergency security zones.
	Coast Guard Integrated Command Center	**C -** Periodic Boadcast Notice to Mariners issued on Channel 16. See Enclosure (X) to Tab A to Appendix 9500.	Within Two Hours of set of higher MARSEC Levels. Additionally within one hour of Marine Events controlled by the Area Maritime Security Plan.
	MJTF Law Enforcement Vessels	**E –** Delivery of appropriate educational and enforcement warnings including non-compliance notices to specific vessels.	During escort and patrol activities afloat.
Evacuation instructions linked to credible threats and/or Transportation Security Incidents that could affect large residential/high-occupancy areas.	County Emergency Operations Centers	**P -** Emergency evacuation/alert phone calls.	In extreme emergencies when the public must be directly informed in order to protect lives, within DHS-established timeframes.
	County Emergency Operations Centers	**A -** Emergency Broadcast System alerts and media releases.	In extreme emergencies when the public must be directly informed in order to protect lives, within DHS-established timeframes.
	Coast Guard Integrated Command Center	**C -** Periodic Boadcast Notice to Mariners issued on Channel 16. See Enclosure (X) to Tab A to Appendix 9500.	In extreme emergencies when the public must be directly informed in order to protect lives, within DHS-established timeframes.
	MJTF Law Enforcement Ashore and Afloat	**E –** Delivery of appropriate evacuation instructions specific areas, vessels, facilities, and individuals	In extreme emergencies when the public must be directly informed in order to protect lives, within DHS-established timeframes.
Incident specific information detailing the nature of the incident and the level of terrorist threat indicated by the incident.	Department of Homeland Security	**P -** Via major media outlets.	Within DHS-established timeframes related to the decision to change the HSAS level.
	JMTX Port Security Committee and Port Canaveral Security Committee	**A -** During public emergency Port Security Committee meetings.	Within 24 hours of the incident.
	Federal Maritime Security Coordinator	**C -** Through Press Releases and statements to the public regarding Coast Guard activities.	Where information and press interest warrangs
	MJTF Law Enforcement Ashore and Afloat	**E –** Delivery of appropriate evacuation instructions specific areas, vessels, facilities, and individuals	In extreme emergencies when the SSI incident specific information must be directly provided in order to protect lives, as soon as possible.

Table 3410.1-2: (U) Communication from the General Public

Information to Communicate	Who communicates	How the Information Is Communicated	When the Information Is Communicated
Reports of Suspicious Activity.	Any member of the general public.	**P** - To the Coast Guard Integrated Command Center (dial **904-247-7318**) and the National Response Center (dial **800-424-8802**)	**24/7 -** As soon as possible upon observing suspicious activity.
		A – To local law enforcement (dial **911**) – request the information be relayed to the Coast Guard.	**24/7 -** As soon as possible upon observing suspicious activity.
		C – To the Coast Guard Integrated Command Center via Fax at 904-XXX-XXXX, 904-XXX-XXXX and 904-XXX-XXXX.	**24/7 -** As soon as possible upon observing suspicious activity.
		E - To the Coast Guard Integrated Command Center via VHF Radio (**Channel 16**).	**24/7 -** As soon as possible upon observing suspicious activity.
Reports of Security Breaches and/or apparent Transportation Security Incidents.	Any member of the general public.	**P** – To local law enforcement (dial **911**), to the Coast Guard Integrated Command Center (dial **904-247-7318**) and the National Response Center (dial **800-424-8802**)	**24/7 -** As soon as possible upon observing the incident or evidence of a security breach.
		A – To the Coast Guard Integrated Command Center via Fax at 904-XXX-XXXX, 904-XXX-XXXX and 904-XXX-XXXX.	**24/7 -** As soon as possible upon observing the incident or evidence of a security breach.
		C – To the Seventh Coast Guard District Command Center at **305-415-6800**.	**24/7 -** As soon as possible upon observing the incident or evidence of a security breach.
		E - To the Coast Guard Integrated Command Center via marine band VHF Radio (**Channel 16**).	**24/7 -** As soon as possible upon observing the incident or evidence of a security breach.
Complaints regarding lack of security, security measures, impact on the general public, or the professionalism of security personnel.	Any member of the general public.	**P -** In writing to Commanding Officer, USCG MSO Jacksonville, 7820 Arlington Expressway, Suite 400, Jacksonville FL 32211-7445.	**24/7 -** As soon as possible
		A – Using the USCG Marine Safety Office Jacksonville web page electronic complaint submission form.	**24/7 -** As soon as possible
		C - Hand deliver correspondence to the U.S. Coast Guard Marine Safety Office – (click here for driving directions).	**24/7 -** As soon as possible
		E – Telephone to the USCG MSO Jacksonville Preparedness Department, 904-232-2640.	During working hours between 0730 a.m. and 1600 p.m. weekdays.
Input on this Area Maritime Security Plan.	Any member of the general public.	**P -** In writing to Commanding Officer, USCG MSO Jacksonville, 7820 Arlington Expressway, Suite 400, Jacksonville FL 32211-7445.	**24/7 -** As soon as possible
		A – Using the USCG Marine Safety Office Jacksonville web page electronic comment submission form. ***(http://www.uscg.mil/d7/units/mso-jax/Readiness & Preparedness/Area_maritime_Security_comments.htm)***	**24/7 -** As soon as possible
		C - Hand deliver correspondence to the U.S. Coast Guard Marine Safety Office – (click here for driving directions).	**24/7 -** As soon as possible
		E – Telephone to the USCG MSO Jacksonville Preparedness Department, 904-232-2640.	During working hours between 0730 a.m. and 1600 p.m. weekdays.

3410.2 (U) Communications with Waterway Users (Boaters)

Communicating security information to waterway users includes many of the processes currently used to identify hazards to navigation or safety related concerns on the MTS.

Table 3410.2-1: (U) Communication to Waterway Users

Information to Communicate	Who communicates	How the Information Is Communicated	When the Information Is Communicated
Maritime Security (MARSEC) level and specific waterway closures linked to the MARSEC level.	Coast Guard Integrated Command Center	**P -** Through electronic distribution of a Marine Safety Information Bulletin (MSIB) via e-mail and posting on the MSO Jacksonville, GRU Mayport, JMTX, and Canaveral Port Authority Internet web pages; a volunteer subscription list is contained in Tab G to Appendix 9500 – interested waterway users may subscribe or delete their addresses from this list on a continuous basis. See Enclosure (X) to Tab A to Appendix 9500.	Within 2 Hours of MARSEC level changes and associated waterway closures.
		A – Through fax distribution of the same Marine Safety Information Bulletin to entities on the volunteer subscription list.	Within 8 Hours of MARSEC level changes and associated waterway closures.
		C - Recurring Boadcast Notice to Mariners issued on Channel 16. See Enclosure (X) to Tab A to Appendix 9500.	Within 2 Hours of MARSEC level changes and associated waterway closures.
	MJTF Law Enforcement and Coast Guard Auxiliary Ashore	**E –** Posting of notices in marinas, yacht clubs, tackle and bait stores, and marine supply shops.	Only when electronic, fax and radio distribution systems are not functional and/or deemed inadequate due to insufficient subscription.
Moving security zones around vessels. Fixed security zones and USACE restricted areas in the Area.	Coast Guard Marine Safety Office Jacksonville and the Government Printing Office (GPO)	**P -** Published in Title 33 Code of Federal Regulations part 165 and the Federal Register.	Before activation for standing security zones and as soon as possible for emergency security zones.
	USCG MSO Jacksonville, GRU Mayport, JMTX, and Canaveral Port Authority	**A –** Graphic diagrams of restricted areas and security zones posted on the Marine Safety Office Jacksonville, Group Mayport, JMTX, and Canaveral Port Authority web pages	Before activation for standing security zones and as soon as possible for emergency security zones.
	Coast Guard Integrated Command Center	**C -** Periodic Boadcast Notice to Mariners issued on Channel 16. See Enclosure (X) to Tab A to Appendix 9500.	Within Two Hours of set of higher MARSEC Levels.
	MJTF Law Enforcement Vessels	**E –** Delivery of appropriate educational and enforcement warnings including non-compliance notices to specific vessels.	During escort and patrol activities afloat.

Table 3410.2-1: (U) Communication to Waterway Users (continued)

Information to Communicate	Who communicates	How the Information Is Communicated	When the Information Is Communicated
Marine Event participation instructions and security restrictions	USCG MSO Jacksonville	**P -** In the publicly available Unclassified version of the Area Maritime Security Plan posted on the Marine Safety Office Jackonville Internet. See the 4000 Series – PREVENTION.	Not later than 01 July 2004 and updated at least annually.
	USCG MSO Jacksonville, GRU Mayport, JMTX, and Canaveral Port Authority	**A –** Published in Title 33 Code of Federal Regulations part 165 and the Federal Register.	Before activation for standing security zones and as soon as possible for emergency security zones.
	Coast Guard Integrated Command Center	**C -** Periodic Boadcast Notice to Mariners issued on Channel 16. See Enclosure (X) to Tab A to Appendix 9500.	Within Two Hours of set of higher MARSEC Levels. Additionally within one hour of Marine Events controlled by the Area Maritime Security Plan.
	MJTF Law Enforcement Vessels	**E –** Delivery of appropriate educational and enforcement warnings including non-compliance notices to specific vessels.	During escort and patrol activities afloat.
Specific security measures all members of the maritime public are expected to execute at each MARSEC Level.	USCG Marine Safety Office Jacksonville	**P -** In the publicly available Unclassified version of the Area Maritime Security Plan posted on the Marine Safety Office Jackonville Internet. See the 4000 Series – PREVENTION.	Not later than 01 July 2004 and updated at least annually.
	USCG MSO Jacksonville, GRU Mayport, JMTX, and Canaveral Port Authority	**A –** Published in Title 33 Code of Federal Regulations part 165 and the Federal Register.	Before activation for standing security zones and as soon as possible for emergency security zones.
	Coast Guard Integrated Command Center	**C -** Periodic Boadcast Notice to Mariners issued on Channel 16. See Enclosure (X) to Tab A to Appendix 9500.	Within Two Hours of set of higher MARSEC Levels.
	MJTF Law Enforcement Ashore and Afloat	**E –** Delivery of appropriate educational and enforcement warnings including non-compliance notices to specific vessels, facilities, and individuals	During security, escort and patrol activities afloat and ashore.

Table 3410.2-2: (U) Communication from Waterway Users

Information to Communicate	Who communicates	How the Information Is Communicated	When the Information Is Communicated
Reports of Suspicious Activity.	Any waterway user or boater	**P** - To the Coast Guard Integrated Command Center (dial **904-247-7318**) and the National Response Center (dial **800-424-8802**)	As soon as possible upon observing suspicious activity.
		A – To local law enforcement (dial **911**) – request the information be relayed to the Coast Guard.	As soon as possible upon observing suspicious activity.
		C – To the Coast Guard Integrated Command Center via Fax at 904-XXX-XXXX, 904-XXX-XXXX and 904-XXX-XXXX.	As soon as possible upon observing suspicious activity.
		E - To the Coast Guard Integrated Command Center via VHF Radio (**Channel 16**).	As soon as possible upon observing suspicious activity.
Reports of Security Breaches and/or apparent Transportation Security Incidents. Reports of hazards to Navigation.	Any waterway user or boater	**P** – To local law enforcement (dial **911**), to the Coast Guard Integrated Command Center (dial **904-247-7318**) and the National Response Center (dial **800-424-8802**)	As soon as possible upon observing the incident or evidence of a security breach.
		A – To the Coast Guard Integrated Command Center via Fax at 904-XXX-XXXX, 904-XXX-XXXX and 904-XXX-XXXX.	As soon as possible upon observing the incident or evidence of a security breach.
		C – To the Seventh Coast Guard District Command Center at **305-415-6800**.	As soon as possible upon observing the incident or evidence of a security breach.
		E - To the Coast Guard Integrated Command Center via VHF Radio (**Channel 16**).	As soon as possible upon observing the incident or evidence of a security breach.
Complaints regarding lack of security, security measures, impact on the general public, or the professionalism of security personnel.	Any waterway user or boater	**P -** In writing to Commanding Officer, USCG MSO Jacksonville, 7820 Arlington Expressway, Suite 400, Jacksonville FL 32211-7445.	As soon as possible
		A – Using the USCG Marine Safety Office Jacksonville web page electronic complaint submission form.	As soon as possible
		C - Hand deliver correspondence to the U.S. Coast Guard Marine Safety Office – (click here for driving directions).	As soon as possible
		E – Telephone to the USCG MSO Jacksonville Preparedness Department, 90**4-232-2640.**	During working hours between 0730 a.m. and 1600 p.m. weekdays.
Input on this Area Maritime Security Plan.	Any waterway user or boater	**P -** In writing to Commanding Officer, USCG MSO Jacksonville, 7820 Arlington Expressway, Suite 400, Jacksonville FL 32211-7445.	As soon as possible
		A – Using the USCG Marine Safety Office Jacksonville web page electronic comment submission form at www.uscg.mil/units[web address].	As soon as possible
		C - Hand deliver correspondence to the U.S. Coast Guard Marine Safety Office – (click here for driving directions).	As soon as possible
		E – Telephone to the USCG MSO Jacksonville Preparedness Department, 904-232-2640.	During working hours between 0730 a.m. and 1600 p.m. weekdays.

3410.3 (U) Communications with Commercial Vessels

Communicating with commercial vessels will require a number of systems that will provide linkages to the large variety of vessels operating within the MTS.

Table 3410.3-1: (U) Communication to Commercial Vessels

Information to Communicate	Who communicates	How the Information Is Communicated	When the Information Is Communicated
Security information relevant to a single vessel.	Coast Guard Integrated Command Center	**P -** Through direct phone contact to the Vessel and Company Security Officer.	As soon as possible after obtaining the security inforemation relevant to a single vessel.
		A – Through the vessel's shipping agents and the bar pilots, relaying the message that the vessel is required to make direct land-line contact with the Coast Guard Integrated Command Center.	When the Company Security Officer confirms he/she cannot make timely contact with the vessel to communicate the information directly.
		C - Through VHF radio contact with the vessel requiring the vessel to make direct land-line contact with the Coast Guard Integrated Command Center.	When the CSO confirms he/she cannot make timely contact..
	MJTF Law Enforcement and Coast Guard Auxiliary Ashore	**E –** Activation of the vessel's GMDSS receiver. Search, location, and delivery in person of appropriate security information to the Vessel Security Officer	Only when all other means of reaching the vessel have failed.
Security information relevant to an entire class or type of vessel (common trade, common ownership, common country-of-origin, etc.)	Commandant of the Coast Guard	**P -** Issuance of a MARSEC Directive and publishing notice of that issuance in the Federal Register.	As soon as possible after obtaining the security inforemation relevant to a class of vessels.
	Coast Guard Integrated Command Center	**A -** Through a limited access meeting to distribute MARSEC Directives - electronic distribution of a notification about the meeting in a Marine Safety Information Bulletin (MSIB) via e-mail and posting on the MSO Jacksonville, GR U Mayport, JMTX, and Canaveral Port Authority Internet web pages; See Tabs A and C to Appendix 9500	Within 2 Hours of receiving a MARSEC Directive or other security information relevant to an entire class of vessels.
		C – Through fax distribution of the same Marine Safety Information Bulletin to entities on the Company and Vessel Security Officers.	Within 8 Hours of receiving the MARSEC directive or other security information.
		E - Through direct phone contact to the Vessel and Company Security Officer.	As soon as possible after obtaining the security inforemation relevant to a class of vessels.
Security information relevant to all commercial vessels (regardless of class or type) within a given geographic region or area.	Coast Guard Integrated Command Center	**P -** Through a limited access meeting to distribute MARSEC Directives - electronic distribution of a notification about the meeting in a Marine Safety Information Bulletin (MSIB) via e-mail and fax; See Tabs A and C to Appendix 9500. Through direct phone contact to the Vessel and Company Security Officers.	As soon as possible after obtaining the security inforemation
		A – Through vessel shipping agents and the bar pilots, relaying the message that the vessel is required to make direct land-line contact with the Coast Guard Integrated Command Center.	When the Company Security Officers confirm they cannot make timely contact with the vessels to communicate the information directly.
		C - Through VHF radio contact with the vessels requiring them to make direct land-line contact with the Coast Guard Integrated Command Center.	When the CSO confirms he/she cannot make timely contact..
	MJTF Law Enforcement and Coast Guard Auxiliary Ashore	**E –** Activation of the vessels' GMDSS receiver. Search, location, and delivery in person of appropriate security information to the Vessel Security Officer	Only when all other means of reaching the vessels have failed.

See Tab B to Appendix 9500 for detailed points fo contact.

3410.4 (U) Communications with Facilities

Communication of security information with regulated and non-regulated facilities will be undertaken using prearranged methods that incorporate communication procedures and methods identified in individual facility security plans.

Table 3410.4-1: (U) Communication to Commercial Shoreline Facilities (RESERVED)

Information to Communicate	Who communicates	How the Information Is Communicated	When the Information Is Communicated
Security information relevant to a single commercial shoreline facility.	Coast Guard Integrated Command Center	**P -** Through direct phone contact to the Facility Security Officer.	As soon as possible after obtaining the security inforemation relevant to a single facility.
		A - Through direct phone contact to the Company Security Officer.	As soon as possible after obtaining the security inforemation relevant to a single facility.
		C – Through the facility's neighbors and landloards, relaying the message that the FSO is required to make direct land-line contact with the Coast Guard Integrated Command Center.	When the Company Security Officer confirms he/she cannot make timely contact with the facilitate to communicate the information directly.
	MJTF Law Enforcement and Coast Guard Auxiliary Ashore	**E –** Delivery in person of appropriate security information to the Facility Security Officer	Only when all other means of reaching the facility have failed.
Security information relevant to an entire class or type of commercial shoreline facility (common trade, common ownership, common vessel-callers, etc.)	Commandant of the Coast Guard	**P -** Issuance of a MARSEC Directive and publishing notice of that issuance in the Federal Register.	As soon as possible after obtaining the sec urity inforemation relevant to a class of facilities.
	Coast Guard Integrated Command Center	**A -** Through a limited access meeting to distribute MARSEC Directives - electronic distribution of a notification about the meeting in a Marine Safety Information Bulletin (MSIB) via e-mail and posting on the MSO Jacksonville, GRU Mayport, JMTX, and Canaveral Port Authority Internet web pages; See Tabs A and C to Appendix 9500	Within 2 Hours of receiving a MARSEC Directive or other security information relevant to an entire class of facilities.
		C – Through fax distribution of the same Marine Safety Information Bulletin to entities on the Company and Facility Security Officers.	Within 8 Hours of receiving the MARSEC directive or other security information.
		E - Through direct phone contact to the Facility and Company Security Officer.	As soon as possible after obtaining the security inforemation relevant to a class of facilities.
Security information relevant to all commercial shoreline facilities (regardless of class or type) within a given geographic region or area.	Coast Guard Integrated Command Center	**P -** Through a limited access meeting to distribute MARSEC Directives - electronic distribution of a notification about the meeting in a Marine Safety Information Bulletin (MSIB) via e-mail and fax; See Tabs A and C to Appendix 9500 . Through direct phone contact to the Facility Security Officers.	As soon as possible after obtaining the security inforemation
		A - Through direct phone contact to the Company Security Officer.	As soon as possible after obtaining the security inforemation relevant to a single facility.
		C – Through the facility's neighbors and landloards, relaying the message that the FSO is required to make direct land-line contact with the Coast Guard Integrated Command Center.	When the Company Security Officer confirms he/she cannot make timely contact with the facilitate to communicate the information directly.
	MJTF Law Enforcement and Coast Guard Auxiliary Ashore	**E –** Delivery in person of appropriate security information to the Facility Security Officers	Only when all other means of reaching the facilities have failed.

See Tab C to Appendix 9500 for detailed points of contact.

3410.5 (U) Communicating with Companies

Communication of security information with Company Security Officers for regulated and non-regulated facilities will be undertaken using prearranged methods that incorporate communication procedures and methods identified in individual facility security plans.

Table 3410.5-1: (U) Communication to Companies. **(RESERVED)**

Information to Communicate	Who communicates	How the Information Is Communicated	When the Information Is Communicated
Security information relevant to a single company.	Coast Guard Integrated Command Center	**P -** Through direct phone contact to the Facility Security Officer.	As soon as possible after obtaining the security inforemation relevant to a single company.
		A - Through direct phone contact to the Company Security Officer.	As soon as possible after obtaining the security inforemation relevant to a single company.
		C – Through the facility's neighbors and landloards, relaying the message that the FSO is required to make direct land-line contact with the Coast Guard Integrated Command Center.	When the ICC cannot make timely contact with the company to communicate the information directly.
	MJTF Law Enforcement and Coast Guard Auxiliary Ashore	**E –** Delivery in person of appropriate security information to the Facility Security Officer	Only when all other means of reaching the company have failed.
Security information relevant to an entire class or type of companies (common trade, common ownership, common vessel-callers, etc.)	Commandant of the Coast Guard	**P -** Issuance of a MARSEC Directive and publishing notice of that issuance in the Federal Register.	As soon as possible after obtaining the security inforemation relevant to a class of companies.
	Coast Guard Integrated Command Center	**A -** Through a limited access meeting to distribute MARSEC Directives - electronic distribution of a notification about the meeting in a Marine Safety Information Bulletin (MSIB) via e-mail and posting on the MSO Jacksonville, GRU Mayport, JMTX, and Canaveral Port Authority Internet web pages; See Tabs A and C to Appendix 9500	Within 2 Hours of receiving a MARSEC Directive or other security information relevant to an entire class of companies.
		C – Through fax distribution of the same Marine Safety Information Bulletin to entities on the Company and Facility Security Officers.	Within 8 Hours of receiving the MARSEC directive or other security information.
		E - Through direct phone contact to the Facility and Company Security Officer.	Only when all other means of reaching the company have failed.
Security information relevant to all companies (regardless of class or type) within a given geographic region or area.	Coast Guard Integrated Command Center	**P -** Through a limited access meeting to distribute MARSEC Directives - electronic distribution of a notification about the meeting in a Marine Safety Information Bulletin (MSIB) via e-mail and fax; See Tabs A and C to Appendix 9500 . Through direct phone contact to the Facility Security Officers.	As soon as possible after obtaining the security inforemation
		A - Through direct phone contact to the Company Security Officer.	As soon as possible after obtaining the security inforemation
		C – Through the facility's neighbors and landloards, relaying the message that the FSO is required to make direct land-line contact with the Coast Guard Integrated Command Center.	When the ICC cannot make timely contact with the company to communicate the information directly.
	MJTF Law Enforcement and Coast Guard Auxiliary Ashore	**E –** Delivery in person of appropriate security information to the Facility Security Officers	Only when all other means of reaching the company have failed.

See Tab D to Appendix 9500 for detailed points fo contact.

3410.6 (U) Role of the Port Security Committees

The AMS Committee's role in communicating security information and procedures is pivotal to ensuring that security information can be quickly and effectively transmitted to a broad range of audiences.

33 CFR 103.310 provides that the Port Security Committees' Executive Subcommittees must serve as a link for communicating threats and changes in MARSEC Levels and disseminating appropriate security information to port stakeholders. As such, the Federal Maritime Security Coordinator will convene Executive Subcommittees (separately or in a joint meeting) to advise and assist the FMSC in the communication of security information. The FMSC may convene the Executive subcommittee to seek advice for the following (this list is not meant to be all-inclusive):

- Identify requirements that will need to be implemented from the AMS Plan when notified of an increase in threat;
- Identify requirements that will need to be implemented from the AMS Plan when notified of a MARSEC Directive;
- Communicate threat information through prearranged procedures to MTS/waterway users;
- To convene a lesson learned/hot wash session to develop measurement and improvement strategies after communication portions of the plan have been implemented.

The Executive Subcommittee members must assist the FMSC with the communication requirements identified in this Plan. 3420 (U) Security Reporting

The National Response Center (NRC) will act as the fusion center for all security information required by 33 CFR Part 101, Subpart C, 101.305. The NRC will receive the reports then act as conduit to consequence mitigation and law enforcement organizations. This includes reporting of suspicious activity and actual breaches in security that does not result in a TSI. These reports and the information garnered as a result of follow on investigation will formulate intelligence and threat information that can be a used to adjust security conditions throughout the country.

3420.1 (U) Procedures for reporting suspicious activity

Suspicious activities will be reported to the NRC and the local authorities. This section defines the procedures for reporting and responding to a report of suspicious activity occuring on the waterways, in the ports, or on the shoreline of Northeast and Eastern Central Florida. Specific Suspicious Activities for which the Port Security Committee has developed reporting and response procedures for two general scenarios. These procedures include unclassified guidelines for the port community and Security Sensitive Information procedures for the Maritime Joint Task Force. Continued development of these Annexes will include Geographically-Specific TSI Response Action Procedures (GSTRAP). The two suspicious activity scenarios include:

(SA-1) Bomb Threat (UNCLAS Annex)
(SA-2) Apparent Surveillance, Access Attempt, Suspicious Boating, Auspicious Divers (UNCLAS Annex)

3420.2 (U) Procedure for Reporting Breaches in

Security

This section defines the procedures for reporting and response to a breach of security occuring on the waterways, in the ports, or on the shoreline of Northeast and Eastern Central Florida. Specific breaches of security for which the Port Security Committee has developed reporting and response procedures for four general scenarios. Continued development of these Annexes will include Geographically-Specific TSI Response Action Procedures (GSTRAP). The four security breach scenarios include:

(SB-1) Trespass Ashore, Stowaway Discovered, or Smallboat in Security Zone (UNCLAS Annex)
(SB-2) Small-scale illegal demonstration (UNCLAS Annex)
(SB-3) Evidence of Tampering w/ Security Systems (UNCLAS Annex)
(SB-4) Security Measures Not in Place (UNCLAS Annex)

3420.3 (U) Procedure for Reporting Transportation Security Incidents (TSIs)

A TSI should be first be reported to the appropriate emergency services (dial 911) to ensure human health and safety measures are taken. Secondary notifications should be made to the Coast Guard Federal Maritime Security Coordinator (dial 904-247-7318 for the Coast Guard Integrated Command Center), then to the National Response Center (dial 1-800-422-8802). This section defines the procedures for reporting and responding to a transportation security incident occuring on the waterways, in the ports, or on the shoreline of Northeast and Eastern Central Florida. Specific TSIs for which the Port Security Committee has developed reporting and response procedures for eleven specific scenarios. Continued development of these Annexes will include Geographically-Specific TSI Response Action Procedures (GSTRAP). The eleven TSI scenarios include:

(TSI-1) Possible or Actual Rogue Vessel (UNCLAS Annex)
(TSI-2) Outbreak of Disease on Vessel (UNCLAS Annex)
(TSI-3) Explosive Device Discovery (UNCLAS Annex)
(TSI-4) Intrusion Ashore w/ small arms (UNCLAS Annex)
(TSI-5) Suspect Cargo including WMD (UNCLAS Annex)
(TSI-6) Suspect Crewmen or Employee (UNCLAS Annex)
(TSI-7) Small Boat Attack (UNCLAS Annex)
(TSI-8) Report of Gunfire in the Port (UNCLAS Annex)
(TSI-9) Explosion (cause unknown), ship or port (UNCLAS Annex)
(TSI-10) Mass Illegal Demonstration (UNCLAS Annex)
(TSI-11) Evacuation of a section of the port (UNCLAS Annex)

3430 (U) Communicating MARSEC Directives

As provided for in Title 33 CFR part 101.405, the Coast Guard may issue MARSEC Directives to provide vessels and facilities nationwide with objective performance standards regarding access control and the secure handling of cargo. These directives will play a vital role in the successful implementation of the MTSA regulations in many ways.

MARSEC Directives allow the Commandant to ensure that there is consistency throughout the country when enforcing the provisions of the MTSA by providing COTPs objective standards by which the performance of vessels and facilities nationwide will be evaluated.

MARSEC Directives allow the Coast Guard the flexibility to tailor objective performance standards to

the prevailing threat environment or industry segment. For example, if high capacity ferry vessels are at a greater risk for a TSI, the Coast Guard may issue a directive that would require enhanced security measures typical of a higher MARSEC Level that would apply only to that segment of the maritime industry.

MARSEC Directives will not impose new requirements, but provide direction to the industry on how to meet the performance standards already required by the regulations. The regulations further provide that the directives will only be issued by Commandant, and only after consultation with other interested Federal agencies within the Department of Homeland Security.

3430.1 (U) Procedures for Communicating Security Directives

When a new MARSEC Directive is issued, the Coast Guard will publish a notice in the Federal Register and announce through other means (i.e. Marine Safety Information Bulletin) that it has issued a new MARSEC Directive. The MARSEC Directives will be individually numbered, and will be assigned to a series that corresponds with the part of this subchapter to which the MARSEC Directive refers. For example, the first MARSEC Directive addressing a new requirement for vessels regulated under part 104 of this subchapter would be identified as MARSEC Directive 104-01.

Upon receiving notice that a new MARSEC Directive has been issued, affected entities must contact the local COTP (if appropriate, their District Commander) to receive a copy of the MARSEC Directive. The COTP or District Commander will confirm, prior to distributing the MARSEC Directive, that the requesting entity is a "covered person" or a person with a "need to know", and that the requesting entity will safeguard the MARSEC Directive as SSI.

Thus, continuing with the example of the previous paragraph, upon receiving notice that a MARSEC Directive in the 104 series has been issued, owners and operators of vessels covered by part 104 of this subchapter need to contact their local COTP to obtain a copy of the MARSEC Directive. They would then be required to comply with the MARSEC Directive, or follow the procedures set out in the MARSEC Directive for gaining approval of an equivalent security measure.

Table 3430.1-1: Dissemination of MARSEC Directives (RESERVED)

Information to Communicate	Who communicates	How the Information Is Communicated	When the Information Is Communicated
An alert that new MARSEC Directives have been published (indicating that port entities need to find out whether they apply or not)	Commandant	**P –** Published notice in the Federal Register (available online at: [web address]	Within 24 hours of issuing the MARSEC Directive.
	Port Security Committee Co-chairs	**A –** E-mail MSIB to mass distribution (all security related entities, government and commercial) directing attention to the Federal Register and announcing dates, times, and locations where the FMSC will be handing out the Directives.	Within 24 hours of Commandant issuing the MARSEC Directive.
	FMSC	**C –** Fax distribution MSIB to port entities (all security related entities) directing attention to the Federal Register and announcing dates, times, and locations where the FMSC will be handing out the Directives.	Within 72 hours of Commandant issuing the MARSEC Directive.
	FMSC	**E –** Phone call to emergency 24-hour contact number informing CSOs, VSOs, and FSOs that the MARSEC Directives have been issued.	Only when specific entities do not come forward to collect a Directive or when the situation is urgent.

The date, time and location of a mass-distribution meeting for a new MARSEC Directive.	FMSC	**P -** E-mail MSIB to mass distribution (all security related entities, government and commercial) directing attention to the Federal Register and announcing dates, times, and locations where the FMSC will be handing out the Directives. May be combined with the alert that the directives were issued.	Within 24 hours of Commandant issuing the MARSEC Directive.
	FMSC	**A -** Fax distribution MSIB to port entities (all security related entities) directing attention to the Federal Register and announcing dates, times, and locations where the FMSC will be handing out the Directives.	Within 72 hours of Commandant issuing the MARSEC Directive.
	Port Security Committees	**C –** Phone-tree notification by members of the Port Security Committee to fellow CSOs, VSOs, and FSOs.	Within 72 hours of Commandant issuing the MARSEC Directive.
	FMSC	**E –** Phone call to emergency 24-hour contact number informing CSOs, VSOs, and FSOs where and when the MARSEC Directives will be distributed.	Only when the Directive is an emergency.
The applicability of a specific new MARSEC Directive to a specific Company or Facility.	FMSC	P -	(RESERVED)
		A -	
		C -	
		E-	
The MARSEC Directive itself.	(RESERVED)	P-	
		A	
		C-	
		E-	

3430.2 (U) Procedures for Responding to MARSEC Directives

Once a MARSEC Directive has been issued it is the responsibility of the affected entities to confirm compliance with the Directive, to the local COTP or District Commander, as appropriate, and specify the method by which the mandatory measures in the directive has been, or will be, met. In some cases recipients may elect to submit proposed equivalent security measures to the local COTP or District Commander, as appropriate, if the recipient is unable to implement the measures mandated in the MARSEC Directive. However, the entity will only be able to propose such alternatives for the length of time specified in the MARSEC Directive, and he/she will be required to implement any alternative measures that the COTP does approve.

Table 3430.2-1: Responding to MARSEC Directives (RESERVED)

Information to Communicate	Who communicates	How the Information Is Communicated	When the Information Is Communicated
Vessel, facility, or other port entitiy has received and acknowledges receiving a MARSEC Directive		P -	
		A -	
		C -	
		E -	
Vessel, facility, or other port entity has complied with the requirements of a MARSEC Directive.		P -	
		A -	
		C -	
		E -	
Vessel, facility, or other port entity has received a		P -	

MARSEC Directive but cannot implement the requirements of the Directive until questions are answered.		A -	
		C -	
		E -	
Vessel, facility, or other port entity has received a MARSEC Directive but cannot implement the requirements of the Directive at all.		P -	
		A -	
		C -	
		E -	
Vessel, facility, or other port entity has received a MARSEC Directive but requests permission from the Federal Maritime Security Coordinator to implement an alternative measure accomplishing the Directive's objective.		P -	
		A -	
		C -	
		E -	
Vessel, facility, or other port entity has received a MARSEC Directive but requests an extension for additional time to implement the specific requirements of the Directive fully.		P -	
		A -	
		C -	
		E -	

WEB PAGE **http://www.uscg.mil/d7/units/mso-jax/Readiness%20&%20Preparedness/Marsec%20Communication_email.htm**

3430.3 (U) Role of the Port Security Committees

[RESERVED]

3440 (U) Communicating MARSEC Levels

MARSEC levels will be set commensurate with the Homeland Security Advisory System (HSAS). The Secretary of Homeland Security sets the HSAS threat condition and only the Commandant will have the authority to change MARSEC levels to match the HSAS.

An exception to this rule is provided for the FMSCs to temporarily raise the MARSEC level in his/her zone to address an immediate threat to the MTS when the immediacy of the threat or incident does not allow time to notify the Commandant. The FMSC will should only exercise this authority in the most immediate and urgent circumstances. Such circumstances would include immediate action to save lives, mitigate great property damage or environmental damage resulting from a TSI and timely prior notification to the Commandant is not possible. If such a circumstance does arise the FMSC must immediately inform the Commandant via the chain of command. The heightened MARSEC level will only continue as long as necessary to address the serious threat which prompted the setting of the raised level.

3440.1 (U) Procedures to Communicate Changes in MARSEC Levels

Table 3440.1-1: Communicating Changes in MARSEC Levels (RESERVED)

Information to Communicate	Who communicates	How the Information Is Communicated	When the Information Is Communicated
Change in MARSEC			

Threat Intel providing MARSEC change			
Security Measures in AMSP			

3440.2 (U) Reporting Attainment of MARSEC Levels

33 CFR Part 104, 105, and 106 require that regulated entities report that they have received notification of changes in MARSEC level and that they have implemented the appropriate measures in accordance with their plan. This will place a great deal of burden on the communication systems in the port.

Table 3440.2-1: Reporting Attainment of MARSEC Level (RESERVED)

Information to Communicate	Who communicates	How the Information Is Communicated	When the Information Is Communicated
Vessel, facility, or other port entity has received and acknowledges receiving a MARSEC change		P -	
		A -	
		C -	
		E -	
Vessel, facility, or other port entity has complied with the requirements of a MARSEC change.		P -	
		A -	
		C -	
		E -	
Vessel, facility, or other port entity has received a MARSEC change but cannot implement the requirements of the Directive until questions are answered.		P -	
		A -	
		C -	
		E -	
Vessel, facility, or other port entity has received a MARSEC change but cannot implement the requirements of the Directive at all.		P -	
		A -	
		C -	
		E -	
Vessel, facility, or other port entity has received a MARSEC change but requests permission from the Federal Maritime Security Coordinator to implement an alternative measure accomplishing the change's objective.		P -	
		A -	
		C -	
		E -	
Vessel, facility, or other port entity has received a MARSEC change but requests an extension for additional time to implement the specific requirements of the change fully.		P -	
		A -	
		C -	
		E -	

3440.3 (U) Role of Area Maritime Security (AMS) Committee

[RESERVED]

3500 (U) Security Sensitive Information

This section governs the designation of information, personnel, maintenance, safeguarding, and disclosure of records and information that has been determined to be Sensitive Security Information (SSI) as defined in para. 3510. This section does not apply to the maintenance, safeguarding, or disclosure of classified national security information, as defined by Executive Order 12968, or to other sensitive unclassified information that is exempt from public disclosure under the Freedom of Information Act. This section is organized as follows:

3510 (U) Information Constituting Security Sensitive Information

General. In accordance with 49 U.S.C. 114(s), SSI is information obtained or developed in the conduct of security activities, including research and development, the disclosure of which has been determined would—

(1) Constitute an unwarranted invasion of privacy (including, but not limited to, information contained in any personnel, medical, or similar file);
(2) Reveal trade secrets or privileged or confidential information obtained from any person; or
(3) Be detrimental to the security of transportation.

Information constituting SSI. Except as otherwise provided in the interest of public safety or in furtherance of transportation security, the following information, and records containing such information, constitute SSI:

(1) **Security programs and contingency plans**. Any security program or security contingency plan issued, established, required, received, or approved by DOT or DHS, including—
  (i) Any vessel, maritime facility, or port area security plan required or directed under Federal law;
  (ii) Any national or area security plan prepared under 46 U.S.C. 70103; and

(iii) Any security incident response plan established under 46 U.S.C. 70104.

(2) **Security Directives**. Any Security Directive or order—
(i) Issued by TSA under § 1542.303, § 1544.305, or other authority;
(ii) Issued by the Coast Guard under the Maritime Transportation Security Act, 33 CFR part 6, or 33 U.S.C. 1221 et seq. related to maritime security; or
(iii) Any comments, instructions, and implementing guidance pertaining thereto.

(3) **Information Circulars**. Any notice issued by DHS or DOT regarding a threat to aviation or maritime transportation, including any—
(i) Information Circular issued by TSA under § 1542.303, § 1544.305, or other authority; and
(ii) Navigation or Vessel Inspection Circular issued by the Coast Guard related to maritime security.

(4) **Performance specifications**. Any performance specification and any description of a test object or test procedure, for—
(i) Any device used by the Federal government or any other person pursuant to any maritime transportation security requirements of Federal law for the detection of any weapon, explosive, incendiary, or destructive device or substance; and
(ii) Any communications equipment used by the Federal government or any other person in carrying out or complying with any maritime transportation security requirements of Federal law.

(5) **Vulnerability assessments**. Any vulnerability assessment directed, created, held, funded, or approved by the DOT, DHS, or that will be provided to DOT or DHS in support of a Federal security program.

(6) **Security inspection or investigative information**. Details of any security inspection or investigation of an alleged violation of aviation or maritime transportation security requirements of Federal law that could reveal a security vulnerability, including the identity of the Federal special agent or other Federal employee who conducted the inspection or audit.

(7) **Threat information**. Any information held by the Federal government concerning threats against transportation or transportation systems and sources and methods used to gather or develop threat information, including threats against cyber infrastructure.

(8) **Security measures.** Specific details of maritime transportation security measures, both operational and technical, whether applied directly by the Federal government or another person, including—
(i) Security measures or protocols recommended by the Federal government;
(ii) Information concerning the deployments, numbers, and operations of Coast Guard personnel engaged in maritime security duties, to the extent it is not classified national security information.

(9) **Security screening information**. The following information regarding security screening under maritime transportation security requirements of Federal law:
(i) Any procedures, including selection criteria and any comments, instructions, and implementing guidance pertaining thereto, for screening of persons, accessible property, checked baggage, U.S. mail, stores, and cargo, that is conducted by the

Federal government or any other authorized person.

(ii) Information and sources of information used by a passenger or property screening program or system, including an automated screening system.

(iii) Detailed information about the locations at which particular screening methods or equipment are used, only if determined by the COTP to be SSI.

(iv) Any security screener test and scores of such tests.

(v) Performance or testing data from security equipment or screening systems.

(vi) Any electronic image shown on any screening equipment monitor, including threat images and descriptions of threat images for threat image projection systems.

(10) **Security training materials**. Records created or obtained for the purpose of training persons employed by, contracted with, or acting for the Federal government or another person to carry out any maritime transportation security measures required or recommended by DHS or DOT.

(11) **Identifying information of certain transportation security personnel**. Lists of the names or other identifying information that identify persons as—

(i) Having unescorted access to a secure area or restricted area of a maritime facility, port area, or vessel or;

(ii) Holding a position as a security screener employed by or under contract with the Federal government pursuant to maritime transportation security requirements of Federal law.

(iii) Holding a position with the Coast Guard responsible for conducting vulnerability assessments, security boardings, or engaged in operations to enforce maritime security requirements or conduct force protection;

(12) **Critical maritime infrastructure asset information**. Any list identifying systems or assets, whether physical or virtual, so vital to the maritime transportation system that the incapacity or destruction of such assets would have a debilitating impact on transportation security, if the list is—

(i) Prepared by DHS or DOT; or

(ii) Prepared by a State or local government agency and submitted by the agency to DHS or DOT.

(13) **Systems security information.** Any information involving the security of operational or administrative data systems operated by the Federal government that have been identified by the DOT or DHS as critical to maritime transportation safety or security, including automated information security procedures and systems, security inspections, and vulnerability information concerning those systems.

(14) **Confidential business information**.

(i) Solicited or unsolicited proposals received by DHS or DOT, and negotiations arising thereof, to perform work pursuant to a grant, contract, cooperative agreement, or other transaction, but only to the extent that the subject matter of the proposal relates to maritime transportation security measures;

(ii) Trade secret information, including information required or requested by regulation or Security Directive, obtained by DHS or DOT in carrying out maritime transportation security responsibilities; and

(iii) Commercial or financial information, including information required or requested by regulation or Security Directive, obtained by DHS or DOT in carrying out maritime transportation security responsibilities, but only if the source of the information does

not customarily disclose it to the public.

(15) **Research and development**. Information obtained or developed in the conduct of research related to maritime transportation security activities, where such research is approved, accepted, funded, recommended, or directed by the DHS or DOT, including research results.

(16) **Other information**. Any information not otherwise described in this section that the DHS determines is SSI under 49 U.S.C. 114(s) or that the Secretary of DOT determines is SSI under 49 U.S.C. 40119. Upon the request of another Federal agency, the DHS or the Secretary of DOT may designate as SSI information not otherwise described in this section.

3520 (U) Covered Persons

Covered person means any organization, entity, individual, or other person described in para. 3520.1. In the case of an individual, covered person includes any individual applying for employment in a position that would be a covered person, or in training for such a position, regardless of whether that individual is receiving a wage, salary, or other form of payment. Covered person includes a person applying for certification or other form of approval that, if granted, would make the person a covered person described in 3520.1

3520.1(U) Designation as a Covered Person.

The following are designated as Covered Persons:

(a) Each owner, charterer, or operator of a vessel, including foreign vessel owners, charterers, and operators, required to have a security plan under Federal or International law.

(b) Each owner or operator of a maritime facility required to have a security plan under the Maritime Transportation Security Act, (Pub.L. 107-295), 46 U.S.C. 70101 et seq., 33 CFR part 6, or 33 U.S.C. 1221 et seq.

(c) Each person performing the function of a computer reservation system or global distribution system for cruise line passenger information.

(d) Each person participating in a national or area security committee established under 46 U.S.C. 70112, or a port security committee.

(e) Each industry trade association that represents covered persons and has entered into a non-disclosure agreement with the DHS or DOT.

(f) DHS and DOT.

(g) Each person conducting research and development activities that relate to maritime transportation security and are approved, accepted, funded, recommended, or directed by DHS or DOT.

(j) Each person who has access to SSI, as specified in para. 3540.

(k) Each person employed by, contracted to, or acting for a covered person, including a

grantee of DHS or DOT, and including a person formerly in such position.

(l) Each person for which a vulnerability assessment has been directed, created, held, funded, or approved by the DOT, DHS, or that has prepared a vulnerability assessment that will be provided to DOT or DHS in support of a Federal security program.

3530 (U) Restrictions on the Disclosure of SSI.

Duty to protect information. A covered person must—

(1) Take reasonable steps to safeguard SSI in that person's possession or control from unauthorized disclosure. When a person is not in physical possession of SSI, the person must store it a secure container, such as a locked desk or file cabinet or in a locked room.

(2) Disclose, or otherwise provide access to, SSI only to covered persons who have a need to know, unless otherwise authorized in writing by the Commandant of the Coast Guard, or the Secretary of DOT.

(3) Refer requests by other persons for SSI to TSA or the applicable component or agency within DOT or DHS.

(4) Mark SSI as specified in para. 3550.

(5) Dispose of SSI as specified in para. 3570.

Unmarked SSI. If a covered person receives a record containing SSI that is not marked as specified in para. 3530, the covered person must—

(1) Mark the record as specified in para. 3550 and

(2) Inform the sender of the record that the record must be marked as specified in para. 3550.

Duty to report unauthorized disclosure. When a covered person becomes aware that SSI has been released to unauthorized persons, the covered person must promptly inform TSA or the applicable DOT or DHS component or agency.

3540 (U) Persons with a Need to Know

General. A person has a need to know SSI in each of the following circumstances:

(1) When the person requires access to specific SSI to carry out maritime transportation security activities approved, accepted, funded, recommended, or directed by DHS or DOT.

(2) When the person is in training to carry out maritime transportation security activities approved, accepted, funded, recommended, or directed by DHS or DOT.

(3) When the information is necessary for the person to supervise or otherwise manage individuals carrying out maritime transportation security activities approved, accepted, funded, recommended, or directed by the DHS or DOT.

(4) When the person needs the information to provide technical or legal advice to a covered person regarding maritime transportation security requirements of Federal law.

(5) When the person needs the information to represent a covered person in connection with any judicial or administrative proceeding, except that in the case of an individual serving as litigation counsel who is not a direct employee of the covered person—

(i) The individual has a need to know only if, in the judgment and sole discretion of the DHS or the Secretary of DOT, access to the SSI is necessary for the litigation

counsel to represent the covered person in the proceeding; and

(ii) The DHS or the Secretary of DOT may make the individual's access to the SSI contingent upon satisfactory completion of a security background check and the imposition of a protective order or agreed upon procedures that establish requirements for safeguarding SSI that are satisfactory to the Administrator or the Secretary of DOT.

Federal employees, contractors, and grantees.
A Federal employee has a need to know SSI if access to the information is necessary for performance of the employee's official duties. A person acting in the performance of a contract with or grant from DHS or DOT has a need to know SSI if access to the information is necessary to performance of the contract or grant.

Need to know further limited by the DHS or DOT. For some specific SSI, DHS or DOT may make a finding that only specific persons or classes of persons have a need to know.

3550 (U) Marking SSI.

Marking of paper records. In the case of paper records containing SSI, a covered person must mark the record by placing the protective marking conspicuously on the top, and the distribution limitation statement on the bottom, of—

(1) The outside of any front and back cover, including a binder cover or folder, if the document has a front and back cover;
(2) Any title page; and
(3) Each page of the document.

Protective marking. The protective marking is: SENSITIVE SECURITY INFORMATION.

Distribution limitation statement. The distribution limitation statement is:

WARNING: This record contains Sensitive Security Information that is controlled under 49 CFR parts 15 and 1520. No part of this record may be disclosed to persons without a "need to know", as defined in 49 CFR parts 15 and 1520, except with the written permission of the Administrator of the Transportation Security Administration or the Secretary of Transportation. Unauthorized release may result in civil penalty or other action. For U.S. government agencies, public disclosure is governed by 5 U.S.C. 552 and 49 CFR parts 15 and 1520.

Other types of records. In the case of non-paper records that contain SSI, including motion picture films, videotape recordings, audio recording, and electronic and magnetic records, a covered person must clearly and conspicuously mark the records with the protective marking and the distribution limitation statement such that the viewer or listener is reasonably likely to see or hear them when obtaining access to the contents of the record.3560 (U) SSI disclosed By TSA or the Coast Guard
General. Except as provided in this section, and notwithstanding the Freedom of Information Act (5 U.S.C. 552), the Privacy Act (5 U.S.C. 552a), and other laws, records containing SSI are not available for public inspection or copying, nor does the Department of Homeland Security release such records to persons without a need to know.

Disclosure under the Freedom of Information Act and the Privacy Act. If a record contains both SSI and information that is not SSI, TSA or the Coast Guard, on a proper Freedom of Information Act

or Privacy Act request, may disclose the record with the SSI redacted, provided the record is not otherwise exempt from disclosure under the Freedom of Information Act or Privacy Act.

Disclosures to committees of Congress and the General Accounting Office. Nothing in this part precludes TSA or the Coast Guard from disclosing SSI to a committee of Congress authorized to have the information or to the Comptroller General, or to any authorized representative of the Comptroller General.

Disclosure in enforcement proceedings.

> **General**. TSA or the Coast Guard may provide SSI to a person in the context of an administrative enforcement proceeding when, in the sole discretion of the DHS or the Commandant of the Coast Guard, as appropriate, access to the SSI is necessary for the person to prepare a response to allegations contained in a legal enforcement action document issued by TSA or the Coast Guard.
>
> **Security background check**. Prior to providing SSI to a person under paragraph (d)(1) of this section, TSA or the Coast Guard may require the individual or, in the case of an entity, the individuals representing the entity, and their counsel, to undergo and satisfy, in the judgment of the DHS or the Commandant of the Coast Guard, a security background check.
>
> **Obligation to protect information**. When an individual receives SSI, that individual becomes a covered person under para. 3520.1 and is subject to the obligations of a covered person under this part.
>
> **No release under FOIA**. When TSA discloses SSI pursuant to this paragraph, TSA makes the disclosure for the sole purpose of providing the information to a person for preparation of a response to allegations contained in a legal enforcement action document. Such disclosure is not a public release of information under the Freedom of Information Act.

Disclosure in the interest of safety or security. The Department of Homeland Security, the Commandant of the Coast Guard, or the Secretary of the Department of Transportation may disclose SSI where necessary in the interest of public safety or in furtherance of transportation security.

3570 (U) Consequences of Unauthorized SSI Disclosure

Violation of this part is grounds for a civil penalty and other enforcement or corrective action by the Department of Homeland Security, and appropriate personnel actions for Federal employees. Corrective action may include issuance of an order requiring retrieval of SSI to remedy unauthorized disclosure or an order to cease future unauthorized disclosure.

3580 (U) Destruction of SSI.

Department of Homeland Security. Subject to the requirements of the Federal Records Act (5 U.S.C. 105), including the duty to preserve records containing documentation of a Federal agency's policies, decisions, and essential transactions, DHS destroys SSI when no longer needed to carry out the agency's function.

Other covered persons. A covered person must destroy SSI completely to preclude recognition or

reconstruction of the information when the covered person no longer needs the SSI to carry out transportation security measures.

Exception. This section does not require a State or local government agency to destroy information that the agency is required to preserve under State or local law.

3590 (U) Procedures for communicating SSI material.

General. SSI material is to be disseminated to Port Security Committee members and/or port stakeholders in accordance with U.S. Coast Guard Commandant Instruction 5510.5. This instruction, in its entirety, has been designated SSI.

Hard Copy Dissemination. Hard copy dissemination may be accomplished via U.S. Mail, interoffice mail, hand carrying within/between buildings; with strict packaging and delivery mandates to ensure privacy.

Electronic Transmission. Electronic transmission of SSI may be accomplished via:

Facsimile. The sender must confirm that the facsimile number of the recipient is current and valid and the facsimile machine is in a controlled area where unauthorized persons cannot intercept the SSI facsimile; or the sender must ensure that an authorized recipient is available at the receiving location to promptly retrieve the information. The information to be transmitted must have a cover sheet that clearly identifies the sender's name and telephone number and contains a warning that, if the message is received by other than the intended recipient, the individual receiving the message must immediately notify the sender for disposition instructions.

Electronic Mail. SSI must be transmitted in a password protected attachment.

Telephone. The caller must ensure that the person receiving the SSI is an authorized recipient. Individuals needing to pass SSI by telephone shall avoid using cellular telephones and cordless telephones unless the circumstances are exigent, or the transmissions are encoded or otherwise protected to reduce the risk of interception and monitoring.

Wireless devices. Do not use cellular phones, pagers, cordless telephones, personal digital assistants to transmit SSI. The risk of interception and monitoring is greater when using wireless devices unless there is an emergency or the transmissions are encrypted.

Internet. Internet posting of SSI is allowed if within a secure socket layer (SSL) with minimum access controls consisting of a user name, password and Primary Content Approval Officials (PCAOs) ensuring that no documents/databases containing SSI information are released. In addition to the SSL and PCAOs, FMSCs may also include SSI warning banners upon logon; Electronically signed non-disclosure agreements at each logon; Limited user permissions (based on need-to-know); and Limitations on storage of SSI information.

3600 (U) Maritime Security Training

Each member of the Port Security Committee is responsible for ensuring those members of their organization directly affected by the execution of the AMS Plan are trained to an appropriate level to execute their roles in implementing the AMS Plan. The Coast Guard will not be involved in any

maritime security training of commercial personnel. However, we can provide a list of maritime security training topics/courses that every person should be familiar with or had some type of training on. In addition, below are several links that will prove beneficial to your training needs.

Hazardous Material I, II, III
Incident Co mmand System (ICS) 100, 200, 300, 400 Level
Explosive & Weapons of Mass Destruction (WMD)

FEMA Education & Training
Florida Emergency Management (Training & Event schedule)
Florida Emergency Management on Terrorism
Florida State Emergency Response Commission
Incident Command System

3700 (SSI) Security Resources

(RESERVED)